IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

BENITA GORGAS and NELSON
GORGAS, individually and on behalf of
similarly situated individuals,

Plaintiffs,

v.

AMAZON.COM, INC.,
AMAZON.COM SERVICES, LLC f/k/a
AMAZON.COM, LLC, and AMAZON
WEB SERVICES, INC.,

Defendants.

No. 22 CV 5159

Judge John J. Tharp, Jr.

<u>MEMORANDUM OPINION AND ORDER</u>

Benita Gorgas and Nelson Gorgas ("the Gorgases"), who are current and former employees of the defendants, respectively, brought this putative class action in the Circuit Court of Cook County, Illinois against Amazon.com, Inc., Amazon.com Services, LLC, and Amazon Web Services, Inc. ("AWS"), alleging that the defendants used cameras to collect their facial geometry scans and thereafter stored, used, profited off, and disclosed the scans in violation of Sections 15(a)-(d) of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (BIPA). Compl., ECF No. 1-1, Exh. A. After the defendants removed the case to this Court, they moved to dismiss the claims for failure to state a claim pursuant to Federal Rule of Civil Procedure 12(b)(6). Having already remanded the Section 15(c) claims to state court, the Court concludes that the complaint sets forth plausible claims under 740 ILCS 14/15(a), (b), and (d), and therefore denies the motion.

BACKGROUND[1]

Benita and Nelson Gorgas worked as Sorting Associates at "two Amazon workplace locations" and at an Amazon "Fulfillment Center," respectively. Compl. ¶¶ 4-5. Amazon[2] required its workers, including the Gorgases, to have electronic images of their faces taken, which were used for identification badges, among other things, and stored in one of Amazon's databases. *Id.* ¶ 7. Further, Amazon uses, markets, and sells to third parties an image-recognition software called Rekognition. *Id.* ¶ 12 (the software's "use cases" include "Searchable Image Library, Face-Based User Verification, Sentiment Analysis, Facial Recognition, and Image Moderation."). Amazon installed thousands of cameras "throughout the facilit[ies]" where the Gorgases worked which identify, detect, monitor, and track workers' movement and behavior for the purposes of "loss prevention, quality assurance, productivity and other things." *Id.* ¶¶ 9-10, 43, 56 (cameras track "how many items were scanned per minute and employees' locations throughout the building"); *see id.* ¶ 58 ("Plaintiffs . . . have been informed that Amazon uses these cameras to track . . . even the amount of time they spend in the restroom."). Using the workplace cameras, coupled with the facial recognition software including Rekognition, Amazon collected, captured, stored, and used biometric identifiers, namely scans of workers' facial geometry. *Id.* ¶¶ 13, 15, 59. Amazon also profits from the Gorgases' biometric data by using it to improve the Rekognition technology and selling the technology to other organizations, and "discloses [the] data to AWS, other Amazon

[1] As with all motions to dismiss, the Court must accept all well-pleaded facts in the complaint as true and draw all permissible inferences in favor of the plaintiffs. *Agnew v. NCAA*, 683 F.3d 328, 334 (7th Cir. 2012).

[2] This background section refers to the three defendants collectively as "Amazon" because that is how the Gorgases refer to the defendants throughout their complaint. Compl. at 1 (defining the three defendants collectively as "Amazon").

entities, and to other, currently unknown, third parties, which, *inter alia*, host and/or analyze the biometric data." *Id.* ¶¶ 16, 46, 60.

Amazon never: (1) informed the Gorgases in writing that their biometric data was being collected, obtained, or stored; (2) informed them in writing of the specific purpose and length of time for which their facial scans and other biometric data were being collected, obtained, stored, and used; (3) developed or adhered to a publicly available retention schedule and guidelines for destroying their facial scans or biometric data; or (4) obtained consent or a written release to collect, obtain, capture, disclose, redisclose, or otherwise disseminate to a third party their biometric data. Compl. ¶¶ 21, 61. Further, it is unclear how long Amazon retains the biometric identifiers and information derived from the capturing of workers' faces, and unclear how long Amazon continues to profit from them. *Id.* ¶ 18. The Gorgases have never been able to find or access, let alone been made aware of, any biometric data retention policy or deletion policies, and no schedules or guidelines were present in onboarding materials or posted on the company intranet or premises. *Id.* ¶¶ 63-67.

DISCUSSION

The Gorgases have alleged that the defendants violated Section 15(a), Section 15(b), and Section 15(d) of BIPA[3], which "imposes numerous restrictions on how private entities collect, retain, disclose and destroy biometric identifiers[.]" *Rosenbach v. Six Flags Entm't Corp.*, 432 Ill. Dec. 654, 656, 129 N.E.3d 1197, 1199 (Ill. 2019); *see also* 740 ILCS 14/10 ("'Biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."). Section 15(a) requires that a private entity "in possession of" biometric data (1) develop a written, publicly

[3] Because the Gorgases' Section 15(c) claims have been remanded to state court, this opinion does not address any argument pertaining to those claims.

available policy that includes a retention schedule and destruction guidelines and (2) permanently destroy data upon the satisfaction of the "initial purpose for collecting or obtaining" it or "within 3 years" of the entity's last interaction with the person, whichever comes first. 740 ILCS 14/15(a). Section 15(b) provides that, prior to collecting biometric data, entities must first (1) inform the person in writing that the information is being collected or stored; (2) state the "specific purpose and length of term for which" the data "is being collected, stored, and used"; and (3) receive a written release from the person. 740 ILCS 14/15(b). Finally, Section 15(d) states that entities in possession of biometric data may only disclose or "otherwise disseminate" a person's data upon obtaining the person's consent or in limited other circumstances inapplicable here. 740 ILCS 14/15(d). BIPA creates a private right of action for "[a]ny person aggrieved by a violation." 740 ILCS 14/20.

The defendants make four arguments pertinent to the Section 15(a), (b), and (d) claims. First, they assert that the complaint should be dismissed because the Gorgases improperly conflate their allegations against all three defendants and fail to distinguish each defendant's conduct, thereby providing insufficient notice regarding the claims against them. Second, and relatedly, they maintain that Amazon.com, Inc. is the parent company of the other defendants and should be dismissed because the Gorgases do not sufficiently allege that it exercised direct control over its subsidiaries. Third, the defendants argue that the Section 15(a), (b), and (d) claims should be dismissed because the Gorgases allege no facts plausibly supporting the conclusion that the defendants "possessed" or "collected" biometric data. Fourth, the Section 15(d) claims should also be dismissed, they say, because the Gorgases allege no facts plausibly supporting the conclusion that the defendants "disclosed" or "disseminated" their data. The Court addresses each argument in turn.

I. Group Pleading

The defendants first argue that the Gorgases impermissibly fail to differentiate among the defendants in their allegations. For example, the defendants point out that "[n]either plaintiff alleges which Amazon Defendant employs them, operates the facilities where they worked, or operates any of the cameras they observed at those facilities." Mot. Dismiss, ECF No. 20 at 4; *see Bank of Am., N.A. v. Knight*, 725 F.3d 815, 818 (7th Cir. 2013) (dismissing the complaint "as a matter of normal pleading standards" because "[a] contention that 'the defendants looted the corporation'—without any details about who did what—is inadequate. . . . Each defendant is entitled to know what he or she did that is asserted to be wrongful. A complaint based on a theory of collective responsibility must be dismissed.").

Group pleading, however, is not per se improper. A complaint survives if any group pleadings, taken along with any individual pleadings, create the plausible inference that each defendant is liable. *Martinez v. Wexford Health Servs., Inc.*, No. 3:18-CV-50164, 2021 WL 1546429, at *3 (N.D. Ill. Apr. 20, 2021) ("On the other hand, if the group allegations, combined with any individual allegations and reasonable inferences, fail to put a specific defendant on notice as to their alleged personal involvement in the injury, the Court must grant that defendant's motion to dismiss.") (citing *Knight*, 725 F.3d at 818). As the cases cited by the defendants indicate, the key is whether the complaint provides sufficient notice to each defendant. *Atkins v. Hasan*, No. 15 CV 203, 2015 WL 3862724, at *2 (N.D. Ill. June 22, 2015); *see Airborne Beepers & Video, Inc. v. AT & T Mobility LLC*, 499 F.3d 663, 667 (7th Cir. 2007) ("at some point the factual detail in a complaint may be so sketchy that the complaint does not provide the type of notice of the claim to which the defendant is entitled under Rule 8.").

The Court finds that the complaint here provides sufficient notice to each defendant, despite employing a consistent "group pleading" approach, because the allegations are directed at all the defendants. Therefore, the defendants do not have to speculate about which claims or allegations pertain to them; they must defend against them all. As the Gorgases argue in their response, the complaint alleges that each defendant engaged in the same behavior of collecting biometric data using cameras and software in Amazon warehouses and subsequently storing, using, profiting from, and disclosing that data. Resp., ECF No. 24 at 1-2 (noting "each Defendant's independent and separate collection" and "distinct and separate role"). Unlike in *Knight*, where the plaintiff alleged without any further elaboration that "the defendants looted the corporation," the Gorgases allege that all defendants took electronic images of their employees' faces, stored them in their databases, used and sold software like Rekognition, installed thousands of cameras and used facial recognition software to identify and track workers' movement, sold the technology to other organizations, and disclosed biometric data to Amazon entities and other third parties which hosted or analyzed the data. All defendants allegedly did so without obtaining any consent from the Gorgases or developing or adhering to a biometric data retention policy. Accordingly, the defendants are not left "in the dark" by "ambiguous formulations of collective action by multiple defendants that fail to 'adequately connect specific defendants to illegal acts.'" *Robles v. City of Chicago*, 354 F. Supp. 3d 873, 875 (N.D. Ill. 2019). It is true, as the defendants point out, that one allegation is unartfully crafted; the Gorgases define "Amazon" to include all three defendants, and thereafter assert that "Amazon disclosed Plaintiffs' sensitive biometric data to AWS . . ." Compl. ¶¶ 46, 60. That allegation is partly illogical, because AWS cannot disclose data to itself, but while inelegant, such an allegation does not doom the complaint or justify dismissal of any claims.

II. Amazon.com, Inc. as Parent Company

The defendants next argue that the Gorgases fail to allege facts supporting the liability of Amazon.com, Inc.—which the defendants assert is the parent company of Amazon.com Services, LLC and AWS[4]—for the purported acts of its subsidiaries. Mot. Dismiss at 7-8 (citing *Forsythe v. Clark USA, Inc.*, 224 Ill. 2d 274, 282, 864 N.E.2d 227, 233 (2007) ("[i]t is a general principle deeply 'ingrained in our economic and legal systems' that a parent corporation is not liable for the acts of its subsidiaries") and *Gass v. Anna Hosp. Corp.*, 392 Ill. App. 3d 179, 185, 911 N.E.2d 1084, 1090 (2009) (corporate veil will be pierced "where the subsidiary is 'so organized and controlled, and its affairs so conducted by a parent, that observance of the fiction of separate identities would sanction a fraud or promote injustice under the circumstances.'")). But the defendants mischaracterize the allegations in the complaint. The Gorgases do not allege conduct by a subsidiary and attempt to hold the parent company liable for that conduct by adding it to the caption of the complaint. Rather, the Gorgases allege that Amazon.com, Inc. and the other defendants engage in the same illegal conduct—namely, using warehouse cameras and facial recognition technology to collect facial geometry and store, use, profit from, and disseminate that data. The Gorgases do not need to pierce the corporate veil to plausibly make those allegations. Of course, discovery may reveal, for example, that the subsidiaries alone controlled or installed all the workplace cameras, but at this stage the Court must accept the well-pleaded allegations as true.

[4] The complaint does not fully confirm the defendants' assertion regarding the defendants' corporate structure, as it fails to allege that Amazon.com, Inc. is the parent company of Amazon.com Services, LLC. Compl. ¶¶ 1-2 ("Amazon.com, Inc. and Amazon.com Services, LLC, commonly known as 'Amazon,' is a leading multinational technology company[.] . . . AWS is a subsidiary of Amazon.com, Inc. and one of the largest platforms and providers of cloud computing services.").

For these reasons, the argument is unpersuasive, and the motion to dismiss Amazon.com, Inc. denied.

III. Sufficiency of Pleading: "Possess" or "Collect"

Third, the defendants contend that the complaint is devoid of factual allegations suggesting that any defendant "possessed" their biometric data, as required under Sections 15(a) and (d), or that any defendant purposefully "collected" biometric data from them, as required under Section 15(b). They characterize the allegations regarding possession or collection of biometric data as speculative legal conclusions, unsupported by underlying facts. Mot. Dismiss at 9 ("Plaintiffs do not . . . allege that they observed anything, read anything, or were told anything suggesting (directly or indirectly) that any Amazon Defendant secretly uses facial recognition technology on images or videos captured by workplace cameras."). The defendants assert that the Gorgases' make an "illogical leap" by concluding that the defendants collect and possess facial geometry scans based upon (1) the presence of cameras in warehouses and (2) defendants' ownership of facial recognition software. *Id.* at 9-10 (citing, among other cases, *Constr. Workers Pension Fund-Lake Cnty. & Vicinity v. Navistar Int'l Corp.*, 114 F. Supp. 3d 633, 644 (N.D. Ill. 2015) (allegations failed "to offer contemporaneous detailed facts supporting the assertions") and *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 286 (N.D. Ill. 2019) (dismissing the Section 15(b) claim against one defendant, Kronos, because the precise allegations made clear that another defendant actually "collected the fingerprints using a system that Kronos supplied to" it)). The Gorgases, predictably, disagree, arguing that their factual allegations are sufficient to state a claim.

The Court agrees with the Gorgases. They do not merely parrot BIPA's statutory language by alleging that the defendants possess and collect biometric data. Instead, they allege that the defendants (1) captured electronic images of the Gorgases' and other workers' faces for badge identification purposes, (2) owned and sold facial recognition technology (including, specifically, Rekognition), and (3) scanned workers' facial geometry using their own facial recognition technology and warehouse cameras, which the Gorgases personally saw throughout the warehouses. Importantly, the Gorgases further allege that they "have been informed that Amazon uses these cameras to track attendance times, including when they enter and leave the Amazon workplace, productivity, loss prevention and even the amount of time they spend in the restroom." Compl. ¶ 58. The Court must accept these facts as true and draw "all reasonable inferences" in the Gorgases' favor, and it does not require an implausible leap to conclude from the above facts that the defendants possess or collect biometric data. *Trexler v. City of Belvidere*, No. 3:20-CV-50113, 2021 WL 243575, at *1 (N.D. Ill. Jan. 25, 2021) (quoting *Calderone v. City of Chicago*, 979 F.3d 1156, 1161 (7th Cir. 2020)). To track their employees so successfully via camera, the defendants would have to hire employees to constantly monitor the camera feeds, or otherwise automate the process with image recognition technology, and the latter can be reasonably inferred. Accordingly, by offering facts by which the Court can reasonably infer that the defendants are liable for the misconduct alleged, the Gorgases distinguish their complaint from those in cases like *Constr. Workers Pension Fund* and *Namuwonge*. Indeed, in contrast to *Namuwonge*, the defendants here are alleged to have directly used cameras and facial recognition technology to collect data, as opposed to having provided a system for collection to a separate company.

IV. Sufficiency of Pleading: "Disclose" or "Disseminate"

Finally, the defendants argue that the Gorgases fail to plausibly allege that any defendant "disclosed" or "disseminated" their biometric data, as Section 15(d) requires. 740 ILCS § 14-15(d) (entity "in possession" of data may not "disclose, redisclose, or otherwise disseminate" that data, absent consent or other limited exceptions). Regarding disclosure or dissemination, the Gorgases allege that "Amazon disclosed Plaintiffs' sensitive biometric data to AWS, other entities, and to other, currently unknown, third parties, which, *inter alia*, host and/or analyze the biometric data." Compl. ¶ 60; *id.* ¶ 46 (Amazon "fails to inform employees that it discloses their sensitive biometric data to AWS, other ***Amazon*** entities, and to other, currently unknown, third parties[.]") (emphasis added). The defendants maintain that these allegations parrot BIPA's statutory language and are not supported by a single fact. *See Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 969 (N.D. Ill. 2020) (dismissing Section 15(d) claim as "rank speculation" because the plaintiff "has not satisfied the court that [the plaintiff] alone has possession of the facts necessary to [the] Section 15(d) claim. If [the plaintiff] has a legitimate reason to suspect that [the defendant] disclosed his biometric data . . . he surely possesses information of some kind that triggered his suspicion—such as reports that [the defendant] has unlawfully disseminated biometric data in the past, or indications that [the plaintiff] or the putative class members experienced identify theft after they used their employers' Pyxis systems."); *Namuwonge*, 418 F. Supp. 3d at 285 (dismissing Section 15(d) claim against Kronos because the claim was based on "speculative allegations," including that Kronos "in turn disclosed her fingerprints to other third parties that host the data," and the plaintiff "did not allege other specifics related to any disclosure by Kronos to a third party").

In response, the Gorgases insist that they "describe the circumstances of a specific, plausible dissemination," presumably referring to their allegation that the defendants disclosed data to AWS and other Amazon entities. Resp. at 12 (quoting *Cothron v. White Castle Sys., Inc.*, 467 F. Supp. 3d 604, 618 (N.D. Ill. 2020) (denying motion to dismiss Section 15(d) claim because the plaintiff "pleaded information that triggered her suspicion" of dissemination by alleging "known involvement of a specific third party in the fingerprint-based system")). They distinguish *Namuwonge* by pointing out that the court there dismissed the Section 15(d) claims without prejudice and with leave to replead. In addition, the Gorgases cite *Figueroa v. Kronos Inc.*, where the court denied the motion to dismiss the Section 15(d) claims after the plaintiff alleged that Kronos disseminated Plaintiffs' biometric data to other firms that hosted the information in their data centers. 454 F. Supp. 3d 772, 779, 785 (N.D. Ill. 2020). Last, the Gorgases argue that it is impossible for them to know exactly to whom the defendants disseminated the data, without the benefit of discovery.

The Gorgases have the better of the argument. True, as the defendants point out, the Gorgases do not plead additional facts supporting their allegations that the defendants disclosed biometric data to unknown third parties, or facts involving any outside third party that would raise their suspicion of dissemination. But they were not required to do so; there is no obligation to plead facts that bear on every statutory element of a claim. *Rowlands v. United Parcel Serv. - Fort Wayne*, 901 F.3d 792, 800 (7th Cir. 2018). Indeed, it is "manifestly inappropriate for a district court to demand that complaints contain all legal elements (or factors) plus facts corresponding to each." *Chapman v. Yellow Cab Coop.*, 875 F.3d 846, 848 (7th Cir. 2017). "It is enough to plead a plausible claim, after which 'a plaintiff receives the benefit of imagination, so long as the hypotheses are consistent with the complaint.'" *Id.* (quoting *Twombly*, 550 U.S. at 563). The Gorgases' dissemination claim is plausible in light of the allegations of unconsented collection and use of facial biometric data in conjunction with improvements to, and marketing of, the Rekognition software. There is no requirement that they specifically allege the identities of third parties to which that data was disseminated.

Nevertheless, the Gorgases allege more than dissemination to unknown third parties. They expressly allege that the defendants also disseminated data ***to AWS and other Amazon entities***. Compl. ¶ 46. In *Cothron*, this Court held that the Section 15(d) claims against White Castle survived where the plaintiff alleged that White Castle used software provided by a specific third party—Cross Match. *Cothron*, 467 F. Supp. 3d at 618. That allegation provided a "basis to suspect" that White Castle had disseminated the data. *Id.*

The same is true here. Given the Gorgases' other allegations, including that each defendant used and sold the Rekognition software and improved that technology through use of the Gorgases' biometric data, the Court finds that the allegations in the complaint give rise to a plausible claim that the defendants disseminated the data amongst themselves and other Amazon entities. The allegations may prove false; for example, it may be the case that each defendant independently collected biometric data without disseminating it. At this stage, however, the Gorgases have alleged enough to plausibly state a Section 15(d) claim.

The defendants argue that, at the very least, the Section 15(d) claims against AWS must be dismissed because AWS cannot disseminate data to itself. But the Gorgases allege that the defendants, including AWS, disseminated data to "other Amazon entities," which could include Amazon.com, Inc., Amazon.com Services, LLC, or others. The argument is therefore without merit. And because the Court finds that the allegations regarding dissemination to AWS and other Amazon entities raise a plausible claim to relief, the Court need not address dismissal of other specific allegations. *See BBL, Inc. v. City of Angola*, 809 F.3d 317, 325 (7th Cir. 2015) ("A motion to dismiss under Rule 12(b)(6) doesn't permit piecemeal dismissals of *parts* of claims; the question at this stage is simply whether the complaint includes factual allegations that state a plausible claim for relief.").

*   *   *

For the foregoing reasons, the motion to dismiss is denied. The plaintiffs’ claims pursuant to 740 ILCS 14/15(a), (b), and (d) will proceed to discovery.

John J. Tharp Jr.

Dated: June 23, 2023

John J. Tharp, Jr.
United States District Judge